Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 438254, 8 pages
http://dx.doi.org/10.1155/2014/438254

Research Article

Secure and Privacy Enhanced Gait Authentication on Smart Phone

Thang Hoang and Deokjai Choi

Department of Electronics and Computer Engineering, Chonnam National University, Gwangju 500-757, Republic of Korea

Correspondence should be addressed to Deokjai Choi; dchoi@jnu.ac.kr

Received 29 January 2014; Accepted 26 February 2014; Published 14 May 2014

Academic Editors: Y. Pan and J. H. Park

Smart environments established by the development of mobile technology have brought vast benefits to human being. However, authentication mechanisms on portable smart devices, particularly conventional biometric based approaches, still remain security and privacy concerns. These traditional systems are mostly based on pattern recognition and machine learning algorithms, wherein original biometric templates or extracted features are stored under unconcealed form for performing matching with a new biometric sample in the authentication phase. In this paper, we propose a novel gait based authentication using biometric cryptosystem to enhance the system security and user privacy on the smart phone. Extracted gait features are merely used to biometrically encrypt a cryptographic key which is acted as the authentication factor. Gait signals are acquired by using an inertial sensor named accelerometer in the mobile device and error correcting codes are adopted to deal with the natural variation of gait measurements. We evaluate our proposed system on a dataset consisting of gait samples of 34 volunteers. We achieved the lowest false acceptance rate (FAR) and false rejection rate (FRR) of 3.92% and 11.76%, respectively, in terms of key length of 50 bits.

1. Introduction

Smart environments established by the development of mobile technology have brought vast benefits to human being [1]. Nowadays, mobile devices could be utilized not only for communication and entertainment but also for transaction [2], personal healthcare [3], or even in emergency situations [4]. As a result, more and more personal data are collected and kept in the mobile device for analysis [5], which would lead to increasing system security and user privacy concerns. Basically, security techniques for authentication and identification are commonly based on password (e.g., OTP [2]), token (e.g., ID cards), or biometric recognition (e.g., iris [6], fingerprint [7], face [8], and gait [9] recognition). Biometric based authentication mechanisms are more convenient in terms of end-user usage viewpoint when comparing with the two remaining methods of password and token. However, using biometric authentication on mobile devices should be considered carefully. Due to the fact that biometrics is unique but fuzzy and revocable, most conventional biometric authentication systems are developed based on pattern recognition and machine learning (PR-ML) algorithms to deal with the natural variations of biometric measurement [6]. Enrollment biometric templates or extracted features are stored under unconcealed form for matching with a new biometric sample to authenticate/identify users. This kind of approaches could leave critical vulnerabilities in terms of system security and user privacy, especially when it is implemented on mobile devices. These devices are easily lost so that an adversary could illegally access the mobile repository to obtain original biometric templates. Since biometrics is tied to unique characteristics of an individual which are hardly changed, the user privacy leak means an adversary could partly or fully determine the user's biometrics. From the viewpoint of system security, a compromise of biometric templates results in everlasting forfeiture. An adversary could utilize compromised templates to thereafter always illegally grant access to sensitive services.

In this paper, we introduce an authentication system based on biometric cryptosystem (BCS) to enhance the system security and user privacy on mobile devices. The biometric modality used in our system is human gait which is collected using an inertial sensor named accelerometer attached to the user's body. This type of sensor has been

utilized to propose motivating applications in smart phones recently [3]. To the best of our knowledge, this is the first approach of a BCS using gait biometrics captured from the accelerometer. We utilize a fuzzy commitment scheme [10] whereby the key, acting as an authentication factor, is biometrically encrypted by the user's gait. The gait sample is merely employed to retrieve the cryptographic key and then be always discarded so that the system security and user privacy are significantly enhanced. Moreover, the system has significant advantages in terms of small storage space and low computational requirements. Therefore, it is more applicable to be deployed directly on mobile devices with limited resources, compared with other PR-ML based systems [9].

The rest of this paper is organized as follows. Section 2 presents the related works. Our proposed system is described in Section 3. Experimental evaluations are presented in Section 4. Finally, Section 5 draws our conclusions.

2. Related Works

To preserve the security and user privacy of biometric authentication systems, various modern approaches have been proposed [11], wherein biometric cryptosystems (BCSs) have attracted much research in recent years. State-of-the-art BCSs which were previously proposed mostly utilize physiological modalities such as iris [12], face [13], and fingerprint [14]. There are some studies that use behavioral biometrics such as signature [15] and voice [16]. Generally, BCSs could be classified into 2 subsystems including key-binding and key-generation systems [11]. In key-binding systems, a random key string is generated and then bound with a biometric template yielding helper data. Such data are stored for further utilization to retrieve the key in the authentication phase. For example, Hao et al. [17] proposed an iris based BCS using fuzzy commitment scheme. They used 2048 bits of iris code combined with concatenated codes and achieved the false acceptance rate (FAR) and false rejection rate (FRR) of 0% and 0.47%, respectively, and the key length of their system is 140 bits. In contrast to key-binding systems—the key generation scheme—helper data is created directly only from the biometric template. Such helper data will associate with a presented query which is sufficiently close to the original template to generate either the unique key string or the original template. Typical techniques of such scheme are fuzzy extractor [18] and secure sketches [19]. Applications of key-generated scheme have already been implemented on iris [12] and voice [16]. Generally, approaches on physiological modalities achieved better results in terms of error rates and security level, compared with behavioral biometric factors. This is due to the fact that physiological modalities such as iris and fingerprint are more robust than behavioral factors which are significantly affected by various conditions. For example, human voice depends on the state of health, gait of individual changes over time, and so forth.

3. The Proposed Method

Figure 1 sketches the specification of our gait based BCS using a fuzzy commitment scheme [10]. In the enrollment phase, gait signal of a user U will be acquired and preprocessed to reduce the influence of the acquisition environment. Feature vectors are extracted in both time and frequency domains and then binarized. After that, a reliable binary feature vector ω is extracted based on determining reliable components. Concurrently, a cryptographic key m, which is generated randomly corresponding to each user, is encoded to a codeword c by using error correcting codes. The fuzzy commitment scheme F computes the hash value of m and a secured δ using a cryptographic hash algorithm h and a binding function, respectively. The helper data which are used to extract reliable binary feature vectors and values of $h(m)$, δ are locally stored for later use in the authentication phase.

In the authentication phase, the user supposed to be U will provide a different gait sample. It is also preprocessed to extract a feature vector and a reliable vector ω' is extracted by using helper data which is previously stored in the enrollment phase. The decoding function f computes the corrupted codeword c' via binding ω' with δ and then retrieves a cryptographic key m' from c' using a corresponding error correcting code decoding algorithm. Finally, the hash value of m' will be matched with $h(m)$ for authentication decision.

3.1. Gait Signal Preprocessing and Segmentation

3.1.1. Data Acquisition. A Google Nexus One smart phone put inside front pocket is employed to collect user gait signal (Figure 2). This discrete time signal is a sequence of combined values of gravity acceleration, ground reaction force, and inertial acceleration which are captured by a built-in 3-dimensional accelerometer during walking. We present the output of this accelerometer as 3-component vectors

$$A = [a_X, a_Y, a_Z], \quad (1)$$

where a_X, a_Y, a_Z represent the magnitude of the acceleration values acting on three directions, respectively.

3.1.2. Data Interpolation. As the accelerometer integrated in mobile devices is power saving and designed to be simpler than standalone sensors, its sampling rate is not stable and entirely depends on mobile OS. The time interval between two consecutive returned samples is not a constant. The sensor only outputs value when the acceleration on 3 dimensions has a significant change. The sampling rate of Google Nexus One used in our study is instable and fluctuates around 27 ± 2 Hz. Therefore, acquired signal is interpolated to 32 Hz using linear interpolation to ensure that the time interval between two sample points will be fixed.

3.1.3. Noise Filtering. When accelerometer samples movement data by user walking, some noises will inevitably be collected. These could be yielded by idle orientation shifts or bumps on the road during walking. Moreover, mobile accelerometer produces numerous noises compared with standalone sensors since its functionality is fully governed by mobile OS layer. Hence, we adopt a multilevel wavelet decomposition and reconstruction method, specifically the

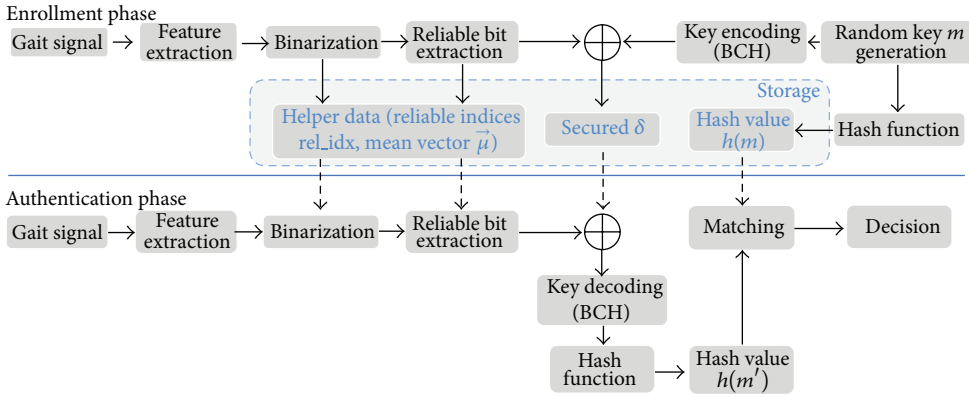
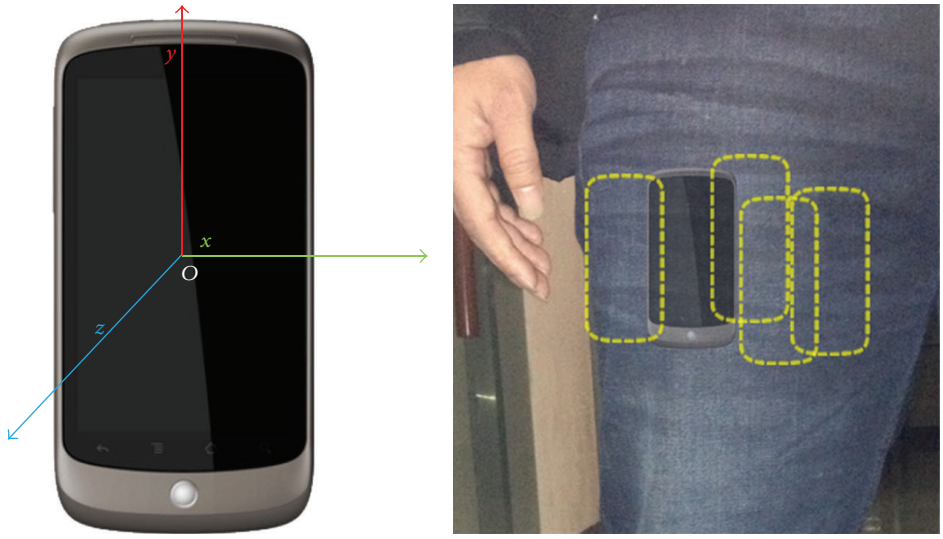


Figure 1: The overall architecture of our proposed gait based BCS using a fuzzy commitment scheme where ⊕ denotes the exclusive-OR operator.



(a) (b)

Figure 2: (a) Google Nexus One phone with a built-in 3-axial accelerometer and (b) the position of device put inside the front trouser pocket.

Daubechies orthogonal wavelet (*Db6*) with level 2, to filter the gait signal. In 1st level, original gait signal is decomposed into two separate parts containing coarse and detail coefficients. Such coarse coefficients acquired in the 1st level are then used as input signal to be decomposed in the next level. This process continues until the desired level is achieved. To eliminate the impacts of noise, in each level, we assign detail coefficients which are lower than a predefined threshold to 0. The noise-filtered signal is reconstructed conversely to the decomposition process, wherein coarse coefficients will associate with new detail coefficients starting from the lowest level until the zero level is achieved.

Because walking is a cyclic activity, we segment a sequence of gait signal after eliminating noise to separate patterns which consist of consecutive gait cycles. A gait cycle is defined as the time interval between two successive occurrences of one of the repetitive events when walking. We observed that whenever the human foot, which is on the same side as the device, touches the ground, the acceleration value in the vertical dimension signal changes obviously as illustrated as red points in Figure 3. We determined these points by calculating the autocorrelation coefficients $A_m = \sum_{i=1}^{N-|m|} x_i x_{i+m}$ on the vertical dimension signal and filtering vivid peaks based on mean and standard deviation. Then based on these points, we segment gait signals into separate patterns, in which each pattern consists of n_{gc} ($n_{gc} = 4$ in our experiment) consecutive gait cycles of all 3 dimensions. Finally, a feature vector is extracted from each pattern in both time and frequency domains.

3.2. Feature Vector Extraction. Denote n_{gc}, N as the number of gait cycles (GC) and the number of acceleration values x in a pattern, respectively. In each pattern, gait features are

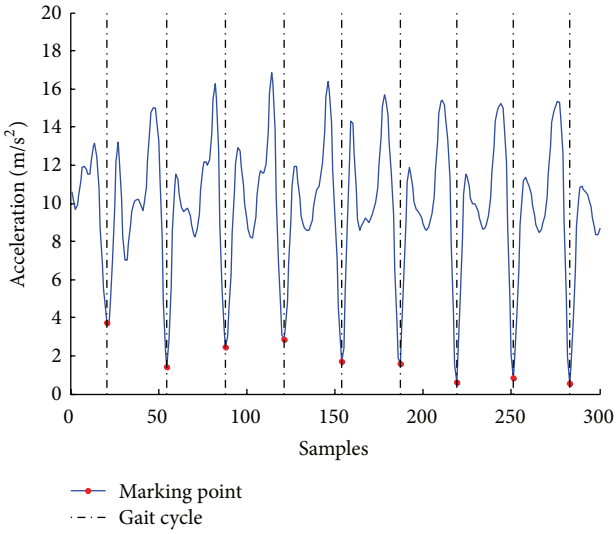


Figure 3: Gait cycle based segmentation on vertical dimension gait signal.

extracted in both time and frequency domains as follows.

(a) Time Domain Features.

(i) Average maximum acceleration

$$\text{avg}_{\max} = \text{mean}\left(\max\left(\text{GC}_i\right)\right)_{i=1}^{n_{\text{gc}}}. \tag{2}$$

(ii) Average minimum acceleration

$$\text{avg}_{\min} = \text{mean}\left(\min\left(\text{GC}_i\right)\right)_{i=1}^{n_{\text{gc}}}. \tag{3}$$

(iii) Average absolute difference

$$\text{avg}_{\text{abs\_dif}} = \sum_{i=0}^{N-1} \left|x_i - \overline{x}\right|. \tag{4}$$

(iv) Root mean square

$$\text{RMS} = \frac{1}{N}\sum_{i=0}^{N-1} x_i^2. \tag{5}$$

(v) 10-bin histogram distribution

$$\text{hd} = \left\langle n_j \right\rangle_0^9 \text{ with } n_j = \frac{\sum_{i=0} x_i}{\text{size}\left(\text{bin}_j\right)}$$
$$\frac{j\left(\max - \min\right)}{10} \le x_i \in \text{bin}_j < \frac{\left(j+1\right)\left(\max - \min\right)}{10}. \tag{6}$$

(vi) Standard deviation

$$\sigma = \sqrt{\left(\frac{1}{N-1}\right)\sum_{i=0}^{N-1}\left(x_i - \overline{x}\right)}. \tag{7}$$

(vii) Waveform length

$$\text{wl} = \sum_{i=1}^{N-1} \left|x_{i+1} - x_i\right|. \tag{8}$$

(viii) Cadence period

$$T_{\text{cad}} = \frac{\sum_i^n t\left(\text{GC}_i\right)}{n}, \tag{9}$$

where $t()$ is the time length of a gait cycle.

(b) Frequency Domain Features.

(i) First 40 FFT coefficients

$$\text{fft} = \left\langle X_k \right\rangle, \quad X_k = \sum_{i=0}^{N-1} x_n e^{-j2\pi ki/N}. \tag{10}$$

(ii) First 40 DCT coefficients

$$\text{dct} = \left\langle X_k \right\rangle,$$
$$X_k = \frac{1}{2}x_0 + \sum_{i=1}^{N-1} x_i \cos\left[\frac{\pi}{N} n\left(k + \frac{1}{2}\right)\right]. \tag{11}$$

Note that each feature in time and frequency domains is extracted on 3 types of acceleration data of Y, Z, M-dimensions, where $a_M = \sqrt{a_X^2 + a_Y^2 + a_Z^2}$, except for the cadence period feature which is extracted based on the timestamp of acquired acceleration values. Totally, we obtain a real-valued feature vector of dimension of $((\text{avg}_{\max} + \text{avg}_{\min} + \text{avg}_{\text{abs\_dif}} + \text{RMS} + \text{hd} + \sigma + \text{wl} + \text{fft} + \text{dct}) \times 3 + T_{\text{cad}}) = ((1 + 1 + 1 + 1 + 10 + 1 + 1 + 40 + 40) \times 3 + 1) = 289$ for each pattern.

3.3. Feature Vector Binarization. We adopt a quantization method which is previously used in [13] for face template binarization. Assume the number of users is denoted by N_u. The number of feature vectors extracted from each user is M. Let $(\vec{T})_{i,j}$ $(i = 1 \cdots N_u, j = 1 \cdots M)$ be the jth feature vector of the user i; the mean over intraclass variability $\vec{\mu}_i$ of the user i is calculated as

$$\vec{\mu}_i = \frac{1}{M}\sum_{j=1}^{M} \vec{T}_j. \tag{12}$$

The mean over all feature vectors $\vec{\mu}$ in the enrollment phase is calculated by

$$\vec{\mu} = \frac{1}{N_u}\sum_{i=1}^{N_u} \vec{\mu}_i. \tag{13}$$

The quantization method transforms tth component in $(\vec{T})_{i,j}$ into $\{0, 1\}$ by comparing tth component of $\vec{\mu}_i$ with a specific threshold defined by corresponding tth component of μ. For each user i, the binary feature vector ω_j is determined by

$$\vec{\omega}_{i,j} = \langle \omega \rangle_t,$$
$$\langle \omega \rangle_t = \begin{cases} 0 & \text{if } \left(\overrightarrow{\mu_l}\right)_t \leq (\vec{\mu})_t \\ 1 & \text{if } \left(\overrightarrow{\mu_l}\right)_t > (\vec{\mu})_t. \end{cases} \quad (14)$$

In the enrollment phase, we use enrollment feature vectors to approximately estimate the value of $\vec{\mu}$. This $\vec{\mu}$ is stored as the helper data and used as the specific threshold for binarizing real-valued feature vectors in the authentication phase.

3.4. Reliable Binary Feature Extraction. As the authors pointed out in [13], when using the quantization method to transform real-valued vectors into the binary forms based on statistical analysis as in the previous section, components in $\vec{\omega}_i$ are significantly instable when using $\overrightarrow{\mu_l}$ and $\vec{\mu}$ to determine the output bit. For example, if the tth component of $(\overrightarrow{\mu_l})_t$ is close to $(\vec{\mu})_t$, the error probability for the next verification will be higher. Therefore, it is necessary to extract only high robust and reliable bits among $\vec{\omega}_i$. First, the variance σ^2 of each tth component for each user i is calculated by

$$\sigma_{i,t}^2 = \frac{1}{M-1} \sum_{j=1}^{M} \left(\left(\vec{T}_{i,j}\right)_t - \left(\overrightarrow{\mu_l}\right)_t \right)^2. \quad (15)$$

Assume that the variability of components is modeled as a Gaussian. Then, the standard error functions of tth bit of the user i are estimated as

$$\text{rel\_val}_i(t) = \frac{1}{2}\left(1 + \text{erf}\left(\frac{\left|\left(\overrightarrow{\mu_l}\right)_t - (\vec{\mu})_t\right|}{\sqrt{2\sigma_{i,t}^2}}\right)\right). \quad (16)$$

Indices of rel_val_i (called rel_idx_i) are also stored as the helper data to extract reliable bits in authentication phase.

3.5. Key Binding Scheme. We adopt the BCH code [20] as an error correcting code to overcome the natural variations between biometric measurements. The advantage of BCH code, compared with other codes, is that it can correct single errors which could occur randomly as in our extracted binary feature vectors. Moreover the decoding process of BCH code is designed to be simple. Therefore, it requires less computational capability and low-powered consumption so that our system is more lightweight to be possibly deployed on mobile devices. Let $\text{BCH}_2(n_c, k, t)$ be a binary BCH code, where n_c is the code length of bits, k is the key length of bits, and t is the error correction capability. The binary cryptographic key m of length k is generated randomly corresponding to each user and then is encoded into the codeword c of length n_c using a $\text{BCH}_2(n_c, k, t)$ encoding scheme [20]. After that, we conceal this c by binding it with the extracted binary feature vector ω yielding a secured δ and then discard ω. Since ω, c are two binary strings, an exclusive-OR operator is adopted to bind these two strings together.

In summary, we represent all of the necessary steps in both enrollment and authentication phases in our system as follows.

Enrollment Phase.

(i) Select a $\text{BCH}_2(n_c, k, t)$ by predefining parameters including the length n_c of the codeword and the length k of the secret key.

(ii) For each user i, real-valued feature vectors $T_i \in \mathbb{R}^{n_r}$ are extracted.

(iii) Determine a mean over all feature vectors $\vec{\mu}$ and extract a binary vector $\omega_i \in \{0, 1\}^{n_r}$ by using the quantization scheme. Then, discard T_i.

(iv) Determine the reliable bit indices rel_idx_i and reduce the length of ω_i to n_c by only selecting first n_c bits among n_r based on rel_idx_i.

(v) Store $\vec{\mu}, \text{rel\_idx}_i$ as helper data for further use to construct new feature vectors in the authentication phase.

(vi) Randomly generate a binary secret key m_i with the length of k.

(vii) Calculate the hash value of m_i by using a cryptographic hash function h (e.g., SHA) and store $h(m_i)$.

(viii) Encode m_i using a $\text{BCH}_2(n_c, k, t)$ encoding scheme to obtain a codeword c_i. Then, discard m_i.

(ix) Bind c_i with ω_i using exclusive-OR operator yielding δ_i. Then, discard ω_i and store δ_i.

Authentication Phase.

(i) For each user i, feature vectors $T_i' \in \mathbb{R}^{n_r}$ are extracted from a new biometric sample.

(ii) Extract binary feature vectors ω_i' with length of n_c with the help of $\vec{\mu}$ and rel_idx_i. Then, discard T_i'.

(iii) Bind ω_i' with the stored δ_i using exclusive-OR operator to obtain a corrupted codeword c_i'.

(iv) Decode c_i' using a BCH decoding scheme to obtain a key m_i' from c_i'.

(v) Calculate hash value $h(m_i')$ using the equivalent cryptographic hash function (e.g., SHA) as in the enrollment phase and then discard m_i'.

(vi) Match $h(m_i)$ with $h(m_i')$; if $h(m_i) = h(m_i')$, the user i is authenticated. Otherwise, he will be rejected.

4. Experiments

4.1. Dataset Description. We evaluate our system on the data collected from a built-in accelerometer in Google Nexus One mobile phone. The sampling rate of the sensor is approximately 27 Hz by setting to SENSOR_DELAY_FASTED mode

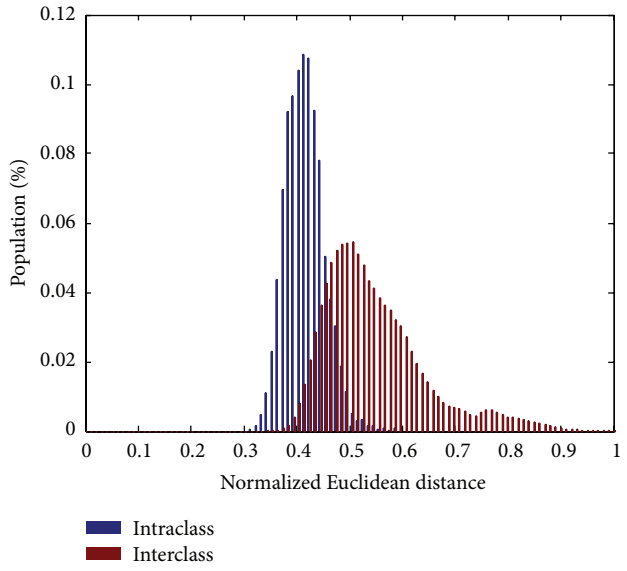


Figure 4: The Euclidean distance of extracted intra- and interclass feature vectors.

on Android SDK. A total of 34 volunteers including 24 males and 10 females with the average age from 24 to 28 participated in our dataset construction. Each volunteer will perform around 18 laps. To make the dataset more realistic, we collect gait signals regardless of footgear and clothes. Volunteers are asked to walk as naturally as possible and change their footgear (e.g., sandal, shoe, or slipper) as well as clothes (e.g., short to long trouser, etc.) whenever they start a new lap. We only have a constraint that when volunteers perform walking, the mobile put in the pocket will not change its position and orientation. To ensure that, we request volunteers to wear trousers having a narrow pocket. Totally, we accumulated the gait signals of 34 volunteers, each having at least 16 real-valued feature vectors which could be extracted using the method in Section 3.2. In our experiment, each volunteer will have an equal number of the extracted feature vectors so that we randomly select 16 vectors for users having more than 16.

4.2. Results. Figure 4 represents the Euclidean distance distribution of extracted real-valued feature vectors. Note that the operation of our BCS is likely to be similar to a threshold-based classification, in which the threshold is likely to be low according to an appropriate distance metric. We can see that the mixing area between intraclass and interclass real-valued feature vectors is large. Thus, applying threshold based classification on these vectors would lead to the high error rate in terms of FAR and FRR. Fortunately, when such vectors are binarized by using the proposed method in Section 3.3, the discrimination of binary feature vectors between users is likely to be higher and the Hamming distance of intraclass feature vectors is getting lower. Figure 5 illustrates the Hamming distance of binary feature vectors of lengths of 127 and 255, respectively. These values of length are selected to be appropriate with the design of the BCH code which allows the length of codeword to be equal to $2^M - 1, M \in \mathbb{N}, M > 3$ and the maximum dimension $d_{\max}$ of feature vector which could be extracted in this study ($d_{\max} = 289$). As already stated, the length of binary feature vector must be equal to the length of BCH codeword for possible binding using an Exclusive-OR operator. Hence, the reliable bit extraction process in Section 3.4 will only select a number of reliable components identical to the codeword length. Looking into Figure 5, we can see that the Hamming distance of intraclass feature vectors of length of 127 is lower than in case of length of 255. We found that this is due to the fact that the actual number of bits being highly reliable according to (16) is just approximately half of the original feature vector dimension. Hence, to obtain a binary feature vector of length of 255, even low reliable bits are also selected.

Table 1: Relative comparison of our proposed system and state-of-the-art BCSs using different schemes of fuzzy commitment scheme (FCS) and fuzzy extractor (FE).

Study	Modality	Scheme	Key size (bits)	FAR (%)	FRR (%)
[13]	Face (CALTECH)	FCS	58	≈0	3.5
	(FERET)		58	≈0	35
[15]	Signature	FCS	29	6.95	6.95
[16]	Voice	FE	30–51	<10	<10
This study	Gait	FCS	55	3.92	11.76
			50	1.4	32.53

Figure 6 illustrates the error rates of our proposed gait based BCS using fuzzy commitment scheme corresponding to two codeword lengths of 127 and 255, respectively. In both cases, when the key length increases which is equivalent to the number of errors allowed in the codeword decreases, the FAR is getting reduced to 0 and the FRR exponentially increases. The best error rates of our proposed system are (1) in the case of codeword length = 127; the achievements of FAR and FRR are approximately 3.921% and 11.76%, respectively, in terms of key length = 50 bits. (2) In the case of codeword length = 255, we achieve the FAR ≈ 1.4% and the FRR ≈ 32.53% in terms of the key length = 55 bits. These keys are rather sufficiently long to be secured by a cryptographic hash algorithm. The FRR of codeword length = 255 is significantly higher than in case of codeword length = 127 because, as already stated, selecting many low reliable bits makes the binary feature vectors of length = 255 more dissimilar. However, the achieved FAR is slightly better (1.4% compared with 3.921%). In both cases, we can see that the FRRs are rather high which could decrease the friendliness of the system. However, user's gait could be captured continuously and implicitly by an accelerometer which does not make the user annoyed as other biometric modalities (e.g., iris, fingerprint, face, and signature). Therefore, this issue is not so considerable.

Table 1 shows the performance of our proposed system compared to some other state-of-the-art BCSs using different behavioral modalities such as voice and signature. Note that all these works use different approaches and the dataset used is totally different so the comparison is just relative. Therefore, through this study, we would merely like to illustrate that

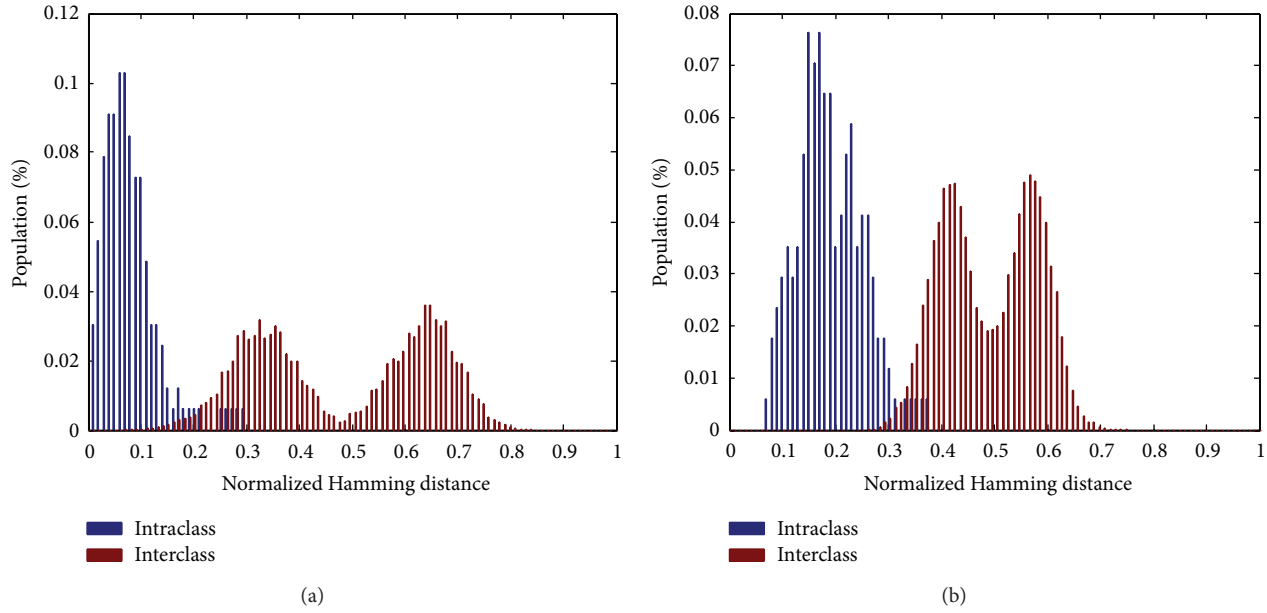


Figure 5: The Hamming distance of intra- and interclass binary vectors of lengths of 127 (a) and 255 (b).

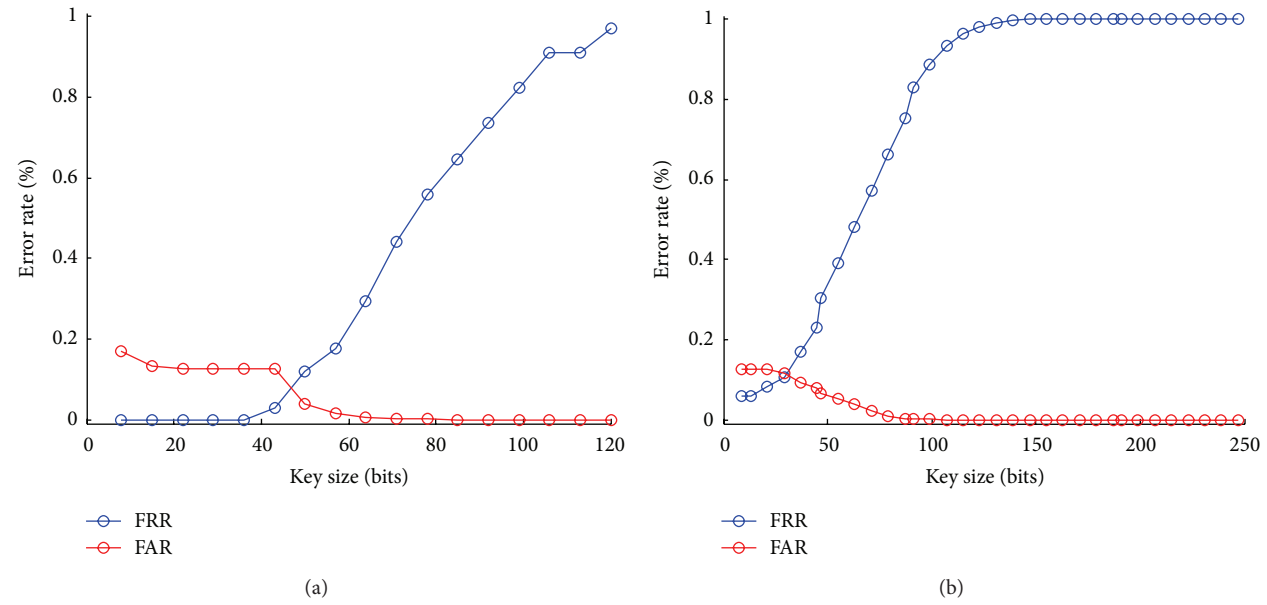


Figure 6: The error rates of FAR and FRR of the key binding result in terms of codeword lengths of 127 (a) and 255 (b).

human gait captured from inertial sensors could be utilized to construct an effective BCS as other behavioral modalities. Moreover due to the fact that we adopt a quantization scheme similar to [13], we also compare our system with this face based BCS. The authors achieved the key length of 58 bits, the FAR of approximately 0%, and the FRR of approximately 3.5% and 35% corresponding to two different datasets of CALTECH and FERET, respectively. We can see that face is a physiological biometric which is more robust than human gait, which is a behavioral modality. Hence, the performance of their system in terms of key length, FAR, and FRR is slightly better.

5. Conclusion

In this paper, we introduce an approach of gait based biometric cryptosystem using fuzzy commitment scheme. The results show a good potential to construct an effective gait based BCS especially on mobile devices. The drawbacks of our work are that the error rates in terms of FAR and FRR are still rather high. We expect to achieve the FAR of 0% to make the system more secured. Hence, our further work will focus on reducing the error rates of FAR and FRR by constructing higher discriminant feature vectors using global feature transformations as well as finding an

optimal quantization scheme for binarization. Moreover, the system security should be analyzed in depth to ensure that a gait based biometric cryptosystem could fulfill the security requirement in order to be deployed in reality. Finally, validating the proposed system on a larger public dataset is also our main further work.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2012R1A1A2007014).

References

[1] J. C. Augusto, V. Callaghan, D. Cook, A. Kameas, and I. Satoh, "Intelligent Environments: a manifesto," *Human-Centric Computing and Information Sciences*, vol. 3, no. 1, pp. 1–23, 2013.

[2] C. L. Tsai, C. J. Chen, and D. J. Zhuang, "Trusted M-banking Verification Scheme based on a combination of OTP and Biometrics," *Journal of Convergence*, vol. 3, no. 3, pp. 23–29, 2012.

[3] J. K. Y. Ng, "Ubiquitous healthcare: healthcare systems and applications enabled by mobile and wireless technologies," *Journal of Convergence*, vol. 3, no. 2, pp. 15–20, 2012.

[4] J. Ahn and R. Han, "An indoor augmented-reality evacuation system for the Smartphone using personalized Pedometry," *Human-Centric Computing and Information Sciences*, vol. 2, no. 1, pp. 1–23, 2012.

[5] T. Teraoka, "Organization and exploration of heterogeneous personal data collected in daily life," *Human-Centric Computing and Information Sciences*, vol. 2, no. 1, pp. 1–15, 2012.

[6] L. Birgale and M. Kokare, "Iris recognition using ridgelets," *Journal of Information Processing Systems*, vol. 8, no. 3, pp. 445–458, 2012.

[7] S. D. Bharkad and M. Kokare, "Hartley transform based fingerprint matching," *Journal of Information Processing Systems*, vol. 8, no. 1, pp. 85–100, 2012.

[8] M. P. Satone and G. K. Kharate, "Face recognition based on PCA on wavelet subband of Average-Half-Face," *Journal of Information Processing Systems*, vol. 8, no. 3, pp. 483–494, 2012.

[9] T. Hoang, T. Nguyen, C. Luong, S. Do, and D. Choi, "Adaptive cross-device gait recognition using a mobile accelerometer," *Journal of Information Processing Systems*, vol. 9, no. 2, pp. 333–348, 2013.

[10] A. Juels and M. Wattenberg, "Fuzzy commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS '99)*, pp. 28–36, November 1999.

[11] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, article 3, 2011.

[12] R. Álvarez Mariño, F. H. Álvarez, and L. H. Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," *Information Sciences*, vol. 195, pp. 91–102, 2012.

[13] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and F. Zuo, "Face biometrics with renewable templates," in *Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072 of *Proceedings of the SPIE*, January 2006.

[14] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes," *Expert Systems with Applications*, vol. 39, no. 7, pp. 6562–6574, 2012.

[15] E. Maiorana, "Biometric cryptosystem using function based on-line signature recognition," *Expert Systems with Applications*, vol. 37, no. 4, pp. 3454–3461, 2010.

[16] B. Carrara and C. Adams, "You are the key: generating cryptographic keys from voice biometrics," in *Proceedings of the 8th International Conference on Privacy, Security and Trust (PST '10)*, pp. 213–222, August 2010.

[17] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[18] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology-Eurocrypt 2004*, pp. 523–540, Springer, Berlin, Germany, 2004.

[19] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in *Advances in Cryptology-ASIACRYPT 2006*, pp. 99–113, Springer, Berlin, Germany, 2006.

[20] R. H. Morelos-Zaragoza, *The Art of Error Correcting Coding*, John Wiley & Sons, Chichester, UK, 2002.